

ABSTRACT

A method for calculating the arithmetic inverse of a number V modulo U , where U is a prime number, that may be used in cryptography, uses a modified extended greatest common divisor (GCD) algorithm that includes a plurality of reduction steps and a plurality of inverse calculations. In this algorithm, the values U and V are assigned to respective temporary variables $U3$ and $V3$ and initial values are assigned to respective temporary variables $U2$ and $V2$. The algorithm then tests a condition and, if the condition tests true, combines multiple ones of the plurality of reduction steps and multiple ones of the inverse calculations into a single iteration of the GCD algorithm.